UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/528,075	09/19/2005	Youdai Watanabe	2611.0233PUS1	2661

2292 7590 06/18/2008
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
SU, SARAH	

ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
06/18/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/528,075	WATANABE, YOUDAI	
	Examiner	Art Unit	
	Sarah Su	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☒ Claim(s) *1-8 and 10-24* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 March 2005* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/17/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 are presented for examination.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

3. The claim for priority from PCT/JP03/11706 filed on 12 September 2003 is duly noted.

Information Disclosure Statement

4. The information disclosure statement filed 17 March 2005 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

5. It is noted that the applicant has indicated that the Uchiyama (CA) reference has been previously cited or submitted to the Office in a prior application relied upon for an earlier filing date under 35 U.S.C. 120. However, the examiner notes that the applicant has not claimed priority to an application filed under 35 U.S.C. 120.

Specification

6. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

7. The disclosure is objected to because of the following informalities:

a. In page 22, line 4: "Fig. 2" should read –Fig. 2A–.

Appropriate correction is required.

Claim Objections

8. Claims 1-8, 10-24 are objected to because of the following informalities:

a. In claim 1, line 38: "the common information (n) is unclear if it relates to "n bits" (claim 1, lines 23 and 31);

b. In claims 2, 4, 6 and 8, line 2: "includes" should read –includes:–;

c. In claim 2, line 6: "approximation," should read –approximation; and–;

d. In claim 3, line 4: "and" should read –; and–;

e. In claim 3, lines 5-6: "a part (k) of pieces of the common information (n)" is unclear if it relates to "a part (k) of pieces of the common information (n)" (claim 1, line 38);

f. In claims 4, 6 and 8, line 3: "apparatus" should read –apparatuses–;

g. In claims 4, 6 and 8, lines 6-7: "a part (k) of pieces of the common information (n)" is unclear if it relates to "a part (k) of pieces of the common information (n)" (claim 1, line 38);

h. In claims 4, 6 and 8, lines 8-9: "a public communication path" is unclear if it relates to "a public communication path" (claim 1, line 29);

i. In claim 5, lines 8-9: "a part (k) of pieces of the common information (n)" is unclear if it relates to "a part (k) of pieces of the common information (n)" (claim 1, line 38);

j. In claim 7, line 6: "a public communication path" is unclear if it relates to "a public communication path" (claim 1, line 29);

k. In claim 7, line 10: "a part (k) of pieces of the common information (n)" is unclear if it relates to "a part (k) of pieces of the common information (n)" (claim 1, line 38);

l. In claim 10, line 4: "approximation," should read –approximation;–;

m. In claim 10, line 7: "procedure, and" should read –procedure; and–;

n. In claim 11, line 4; claim 13, line 7: "and" should read –; and–;

o. In claim 11, lines 5-6; claim 13, lines 8-9: "a part (k) of pieces of the common information (n)" is unclear if it relates to "a part (k) of pieces of the common information (n)" (claim 9, lines 19-20);

p. In claims 12, 14 and 16, lines 3-4: "a part (k) of pieces of the common information (n)" is unclear if it relates to "a part (k) of pieces of the common information (n)" (claim 9, lines 19-20);

q. In claim 15, lines 5-6: "a public communication path" is unclear if it relates to "a public communication path" (claim 9, line 18);

r. In claim 15, lines 9-10: "a part (k) of pieces of the common information (n)" is unclear if it relates to "a part (k) of pieces of the common information (n)" (claim 9, lines 19-20);

s. In claim 17, line 13: "reception data" is unclear if it relates to "reception data" (claim 17, line 7);

t. In claim 18, line 5: "approximation," should read –approximation;–;

u. In claim 18, line 8; claim 19, line 4; claim 21, line 7: "and" should read –; and–;

v. In claim 19, lines 5-6; claim 21, lines 8-9; claim 23, lines 8-9: "a part (k) of pieces of the common information (n)" is unclear if it relates to "a part (k) of pieces of the common information (n)" (claim 17, lines 17-18);

w. In claims 20, 22 and 24, lines 3-4: "a part (k) of pieces of the common information (n)" is unclear if it relates to "a part (k) of pieces of the common information (n)" (claim 17, lines 17-18);

x. In claim 23, lines 5-6: "a public communication path" is unclear if it relates to "a public communication path" (claim 17, lines 14-15);

Appropriate correction is required.

Drawings

9. Figure 9 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g).

10. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because:

a. reference characters "10" and "30" have both been used to designate PARITY CHACK MATRIX CREATION UNIT (Figures 1 and 7);

b. reference characters "11" and "31" have both been used to designate RANDOM NUMBER GENERATION UNIT (Figures 1 and 7);

c. reference characters "13" and "34" have both been used to designate PUBLIC COMMUNICATION PATH COMMUNICATION UNIT (Figures 1 and 7);

d. reference characters "15" and "35" have both been used to designate COMMON KEY CREATION UNIT (Figures 1 and 7);

e. reference characters "S1" and "S11" have both been used to designate CREATE H, G, G^{-1} (Figures 2A and 2B).

11. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 1a (Figure 7).

12. The drawings are objected to because "PARITY CHACK MATRIX CREATION UNIT (Items 10 and 30 in Figures 1 and 7) should read –PARITY CHECK MATRIX CREATION UNIT–.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

13. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

14. Claims 10 and 18 are rejected under 35 U.S.C. 101 because the claimed invention is not supported by either a specific and substantial asserted utility or a well established utility.

Claims 10 and 18 are directed toward an apparatus and a method, which are different statutory categories. This makes the utility for these claims ambiguous and thus they lack a specific and substantial utility. See MPEP § 2173.05(p).

Claims 10 and 18 are also rejected under 35 U.S.C. 112, first paragraph. Specifically, since the claimed invention is not supported by either a specific and substantial asserted utility or a well established utility for the reasons set forth above, one skilled in the art clearly would not know how to use the claimed invention.

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

17. Claims 1, 3-6, 9, 11-14, 17, 19-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Berzanskis et al. (US 2006/0059343 A1 and Berzanskis hereinafter) in view of Yamazaki (Institute of Electronics, Information and Communication Engineers Society Conference 2001).

As to claims 1, 9 and 17, Berzanskis discloses a system and method for key expansion for quantum key distribution, the system and method having:

a photon transmission step of the first communication apparatus transmitting a photon onto the quantum communication path while the photon is in a quantum state specified by a combination of the transmission data and the transmission code (0005, lines 3-4, 9-10)**;**

a photon reception step of the second communication apparatus measuring the photon transmitted on the quantum communication path to obtain reception data specified by the combination of the reception code and measurement result (0005, lines 3-4, 9-10)**;**

a data deletion step of each of the first communication apparatus and the second communication apparatus deciding whether the measuring has been performed with an appropriate measuring apparatus (i.e. same phase-encoding basis)**, saving the reception data of n bits if the measuring has been performed with the appropriate measuring apparatus and transmission data that corresponds to the reception data, and discarding other pieces of the data** (0008, lines 1-6)**;**

a cryptographic key creation step of each of the first communication apparatus and the second communication apparatus discarding a part (k) of pieces of the common information (n) after correction according to public error correction information (0038, lines 6-7), **creating a cryptographic key using information that has remained after discarding, and setting the cryptographic key as a common key which is shared between apparatuses** (0042, lines 4-7)**.**

Berzanskis does not disclose:

a check matrix creation step of each of the first communication apparatus and the second communication apparatus creating the same parity check matrices H(n×k);

a random number generation step of the first communication apparatus generating a random number sequence (transmission data) and randomly determining a predetermined transmission code (base) by the first communication apparatus, and the second communication apparatus randomly determining a predetermined reception code (base);

an error correction information notification step of the first communication apparatus notifying the second communication apparatus through a public communication path of error correction information of k bits based on the parity check matrix H and the transmission data of n bits;

an error correction step of the second communication apparatus correcting the error of the reception data based on the parity check matrix H, the reception data of n bits, and the error correction information.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Berzanskis, as evidenced by Yamazaki. Yamazaki discloses a system and method for error correcting codes for quantum key distribution, the system and method having:

a check matrix creation step of each of the first communication apparatus and the second communication apparatus creating the same parity check matrices H(n×k) (page 5, lines 10-12)**;**

a random number generation step of the first communication apparatus generating a random number sequence (transmission data) and randomly determining a predetermined transmission code (base) by the first communication apparatus, and the second communication apparatus randomly determining a predetermined reception code (base) (page 2, lines 14-16)**;**

an error correction information notification step of the first communication apparatus notifying the second communication apparatus through a public communication path of error correction information of k bits based on the parity check matrix H and the transmission data of n bits (page 4, lines 20-24; page 5, lines 21-24)**;**

an error correction step of the second communication apparatus correcting the error of the reception data based on the parity check matrix H, the reception data of n bits, and the error correction information (page 5, lines 1-6).

Given the teaching of Yamazaki, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Berzanskis with the teachings of Yamazaki by using a check matrix to perform error correction and determine which bits to save. Yamazaki recites motivation by disclosing that performing correction on blocks using a check matrix would solve the problem of frequent communications and a reduced key generation rate (page 2, lines 2-5). It is obvious that the teachings of Yamazaki would have improved the teachings of Berzanskis by using a check matrix to perform error correction on blocks in order to reduce the time required for error correction.

As to claims 3, 11 and 19, Berzanskis discloses:

the cryptographic key creation step includes discarding a part (k) of pieces of the common information (n) by the inverse matrix G^{-1} (0038, lines 6-7).

Berzanskis does not disclose:

wherein the check matrix creation step includes creating an inverse matrix G^{-1} (n×(n-k)), which satisfies G^{-1}·G=I (unit matrix), from a creation matrix G((n-k)×n) satisfying "HG=0,".

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Berzanskis, as evidenced by Yamazaki. Yamazaki discloses:

> **wherein the check matrix creation step includes creating an inverse matrix G^{-1} (n×(n-k)), which satisfies G^{-1}·G=I (unit matrix), from a creation matrix G((n-k)×n) satisfying "HG=0,"** (page 4, lines 10-11; page 5, line 10).

Given the teaching of Yamazaki, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Berzanskis with the teachings of Yamazaki by creating a check matrix by using an inverse matrix. Yamazaki recites motivation by disclosing that the receiver can use the sender's block parity to decode a message if the sender's and receiver's blocks contain different parities (page 4, lines 3-8). It is obvious that the teachings of Yamazaki would have improved the teachings of Berzanskis by creating a check matrix from an inverse matrix in order to allow a receiver to use a sender's block parity if the sending and receiving parities are different.

As to claims 5, 13 and 21, Berzanskis discloses:

> **the cryptographic key creation step includes discarding a part of pieces of the common information (n) by the mapping F** (0038, lines 6-7).

Berzanskis does not disclose:

> **wherein the check matrix creation step includes creating a mapping F to map an n-dimensional vector to an m-dimensional vector (m ≤ n-k), the**

mapping F being one in which the number of elements of a reverse image $(F \cdot G)^{-1}$ (v) in a composition mapping FG of the mapping F and the creation matrix G satisfying "HG=0" is independent of an arbitrary m-dimensional vector v and is constant (2^{n-k-m}).

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Berzanskis, as evidenced by Yamazaki. Yamazaki discloses:

> **wherein the check matrix creation step includes creating a mapping F to map an n-dimensional vector** (i.e. code) **to an m-dimensional vector (m ≤ n-k)** (i.e. block)**, the mapping F being one in which the number of elements of a reverse image $(F \cdot G)^{-1}$ (v) in a composition mapping FG of the mapping F and the creation matrix G satisfying "HG=0" is independent of an arbitrary m-dimensional vector v and is constant (2^{n-k-m})** (page 3, lines 12-14, 19-21; page 4, lines 8-11)**.**

Given the teaching of Yamazaki, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Berzanskis with the teachings of Yamazaki by creating a check matrix by mapping. Yamazaki recites motivation by disclosing that the block size is based on the code size in order to ensure that each block contains a single error for correction (page 3, lines 12-20). It is obvious that the teaching of Berzanskis would have benefited from the teachings of Yamazaki by using a check matrix by relating a code to a block so that each block will have one error for correction.

As to claims 4, 6, 12, 14, 20 and 22, Berzanskis discloses:

one of the communication apparatus, out of the first communication apparatus and the second communication apparatus, creating a nonsingular random matrix R((n-k)×(n-k)) (i.e. M) **to act on the cryptographic key after discarding a part (k) of pieces of the common information (n)** (i.e. corrected) **and informing the nonsingular random matrix R to other one of the communication apparatuses through a public communication path** (0008, lines 16-17; 0042, lines 4-6),

the first communication apparatus and the second communication apparatus using the nonsingular random matrix R to create the cryptographic key (0042, lines 4-9).

18. Claims 2, 7-8, 10, 15-16, 18, 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Berzanskis in view of Yamazaki as applied to claims 1, 9 and 17 above, and further in view of Kou et al. (IEEE Globecom and Kou hereinafter) and Chung et al. (IEEE Transactions on Information Theory and Chung hereinafter).
As to claims 2, 10 and 18, Berzanskis in view of Yamazaki does not disclose:

weight searching step of using finite affine geometry as a basic matrix and searching optimum row and column weight distributions of the parity check matrix by performing optimization of Gaussian approximation,

dividing step of dividing randomly the row and column weights of the finite affine geometry based on the optimum weight distribution by a predetermined procedure, and creating the parity check matrix H of a low-density parity check code in which both the row and column weights or one of the row and column weights is not uniform.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Berzanskis in view of Yamazaki, as evidenced by Chung.

Chung discloses a method for sum-product decoding of low-density parity check codes using a Gaussian approximation, the method having:

weight searching step of using finite affine geometry as a basic matrix and searching optimum row and column weight distributions of the parity check matrix by performing optimization of Gaussian approximation (col. 17, lines 2-3; col. 18, lines 28-32) in order to provide for a simple way to estimate thresholds for low density parity check codes, as recited in Chung (col. 2, lines 38-43).

Berzanskis in view of Yamazaki and Chung does not disclose:

dividing step of dividing randomly the row and column weights of the finite affine geometry based on the optimum weight distribution by a predetermined procedure, and creating the parity check matrix H of a low-density parity check code in which both the row and column weights or one of the row and column weights is not uniform.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Berzanskis in view of Yamazaki and Chung, as evidenced by Kou.

Kou discloses a system and method for low density parity check codes based on finite geometries, the system and method having:

> **dividing step of dividing randomly the row and column weights of the finite affine geometry based on the optimum weight distribution by a predetermined procedure, and creating the parity check matrix H of a low-density parity check code in which both the row and column weights or one of the row and column weights is not uniform** (col. 7, lines 37-41; col. 8, lines 1-8).

Given the teaching of Kou, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Berzanskis in view of Yamazaki and Chung with the teachings of Kou by randomly splitting the row and column weights. Kou recites motivation by disclosing that the parity check code can be extended by splitting the columns which results in a smaller density new code (col. 7, lines 27-31). It is obvious that the teachings of Kou would have improved the teachings of Berzanskis in view of Yamazaki and Chung by splitting the rows and columns in order to produce new check codes with smaller densities

As to claims 7, 15 and 23, Berzanskis in view of Yamazaki and Chung do not disclose:

performing random permutation to the column of the parity check matrix H, selecting specific "1" in the first column of finite affine geometry AG(2,2^S) of a creation element of the parity check matrix H, exchanges a position of "1" through a public communication path, specifying the position (column) after the division corresponding to "1" from the parity check matrix after the random permutation and the position (column) after the division corresponding to "1" in each cyclically shifted column, and discarding a part (k) of pieces of the common information (n) corresponding to the specified position (column).

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Berzanskis in view of Yamazaki and Chung, as evidenced by Kou.

Kou discloses:

performing random permutation to the column of the parity check matrix H, selecting specific "1" in the first column of finite affine geometry AG(2,2^S) of a creation element of the parity check matrix H, exchanges a position of "1" through a public communication path, specifying the position (column) after the division corresponding to "1" from the parity check matrix after the random permutation and the position (column) after the division corresponding to "1" in each cyclically shifted column, and discarding a part (k) of pieces of the common information (n)

corresponding to the specified position (column) (col. 7, lines 37-41; col. 8, lines 1-8)**.**

Given the teaching of Kou, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Berzanskis in view of Yamazaki and Chung with the teachings of Kou by changing the columns of a check matrix. Please refer to the motivation recited above in respect to claims 2, 10 and 18 as to why it is obvious to apply the teachings of Kou to the teachings of Berzanskis in view of Yamazaki and Chung.

As to claims 8, 16 and 24, Berzanskis, combined with Yamazaki, Chung and Kou, discloses:

one of the communication apparatus, out of the first communication apparatus and the second communication apparatus, creating a nonsingular random matrix R((n-k)×(n-k)) (i.e. M) **to act on the cryptographic key after discarding a part (k) of pieces of the common information (n)** (i.e. corrected) **and informing the nonsingular random matrix R to other one of the communication apparatuses through a public communication path** (0008, lines 16-17; 0042, lines 4-6)**,**

the first communication apparatus and the second communication apparatus using the nonsingular random matrix R to create the cryptographic key (0042, lines 4-9)**.**

Prior Art Made of Record

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Lo et al. (US Patent 5,732,139) discloses a system and method for quantum cryptography with reduced data loss.

b. Mazourenko et al. (US Patent 6,272,224 B1) discloses a system and method for quantum distribution of an encryption key.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2131

/Christopher A. Revak/
Primary Examiner, Art Unit 2131